UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Three (3) Facebook accounts, hosted at premises controlled by Facebook, Inc., located at 1601 Willow Road, Menlo Park, CA, more fully described in Attachment A

Case No. MJ20-753

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Three (3) Facebook accounts, hosted at premises controll, more fully described in Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, for a list of information to be disclosed, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371, 1029, 1343, 1344,	Conspiracy, Access Device Fraud, Wire Fraud, and Bank Fraud
18 U.S.C. §§ 1349, 1028A(a)(1)	Conspiracy to Commit Wire/Bank Fraud, and Aggravated Identity Theft

The application is based on these facts:

✓ See Affidavit of Special Agent Michael Spiess, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Michael A. Spiess
Applicant's signature

Michael A. Spiess, Special Agent
Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
○ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/20/2020

Paula L. McCandlis
Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT MICHAEL SPIESS

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Michael Spiess, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the USSS and have been since September 22, 2002. I am currently assigned to the Seattle Field Office, as a Senior Special Agent. I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the USSS Special Agent Training Program located in Beltsville, Maryland. Before becoming a Special Agent, I was employed with the USSS as a Uniformed Officer in Washington, D.C. Before that, I served as a United States Immigration Inspector in Toronto, Canada. I have a Bachelor of Arts Degree from Daemen College in Amherst, New York. In the course of my official duties as a Special Agent, I have investigated a broad range of financial crimes involving credit card fraud, bank fraud, access device fraud, money laundering, wire fraud, cryptocurrency and counterfeit currency and securities. As a result, I have experience with various methods and practices used by criminals to defraud merchants, banks and other financial institutions, including through various types of account takeover schemes and counterfeit checks, both commercial and personal.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for information associated with the following accounts (collectively referred to as the "SUBJECT ACOUNTS"), which are stored at premises controlled by Facebook, Inc. ("Facebook"), an electronic communications service and/or remote computing service provider headquartered in Menlo Park, California:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. The account bearing the profile name "Kev Jones" and accessible at the internet address https://www.facebook.com/Kpremium (hereinafter "**SUBJECT ACCOUNT 1**").

b. The account bearing the profile name "September Love" and accessible at the internet address https://www.facebook.com/september.love.148 (hereinafter "**SUBJECT ACCOUNT 2**").

c. The account bearing the profile name "September Grubb (Queen Naundi)" and accessible at the internet address https://www.facebook.com/SeptySuchALady (hereinafter the "**SUBJECT ACCOUNT 3**").

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Facebook to disclose to the government copies of the information (including the content of communications) relating to the SUBJECT ACCOUNTS, as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review this information to locate the items described in Section II of Attachment B.

4. The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrants in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the United States Secret Service may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft), will be found in the SUBJECT ACCOUNTS. In addition, and as discussed below, there is probable cause to believe that the SUBECT ACCOUNTS were used in furtherance of the criminal scheme under investigation.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience and that of other experienced investigators, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i), and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

STATEMENT OF PROBABLE CAUSE

A. Summary

8. Since in or around 2019, acting on a referral, the USSS and the Kirkland Police Department ("Kirkland PD") have investigated a fraud scheme committed against the Washington-based financial institution Boeing Employees Credit Union ("BECU"), as well

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

as certain BECU accountholders. According to publicly available records, including BECU's website, BECU is a member-owned not-for-profit credit union, which qualifies as a "financial institution" under Title 18, United States Code, Section 20. BECU offers individuals and entities banking services (e.g., checking accounts, savings accounts, credit cards), certificates of deposit, retirement accounts, loans, investment services, and other financial services commonly offered by banks and credit unions.

9. According to BECU, BECU investigators discovered that, between in or about May 2019 and in or about October 2019, approximately twenty-two (22) accounts had been accessed, fraudulently and without authorization, and drained of their funds. More specifically, BECU investigators discovered that one or more individuals (a) called BECU's customer-service representatives, (b) fraudulently posed as real accountholders by presenting stolen personal identifying information (e.g., social-security numbers, mothers' maiden names), (c) obtained information about the victim accounts' prior account activity, (d) successfully requested increases on BECU-imposed limits on withdrawals from automated teller machine ("ATM") and limits on purchases at point-of-sale ("POS") terminals. When requesting these ATM and POS limits, the perpetrators of the fraud fraudulently represented to BECU customer-service representatives that they sought the additional funds in order to purchase vehicles. In certain cases, the perpetrators also entered BECU branch offices, posed as the victim accountholders, claimed that they had lost their debit cards, and fraudulently induced the bank tellers at those BECU branch offices to issue new debit cards in the victim accountholders' names.[1] Through the scheme, the perpetrators were able to steal more than $230,000 from the victim accounts, typically by withdrawing funds from BECU ATMs, and by making purchases at POS terminals at Fred Meyer grocery stores located in King County and Pierce County.

[1] BECU captured surveillance footage of some of the ATM withdrawals, which helped identify some of the subjects described below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. BECU's Identification of Employee SEPTEMBER GRUBB

10. BECU reported to law enforcement that its investigators had identified a BECU employee named SEPTEMBER GRUBB ("GRUBB") as a perpetrator of the scheme, and a potential singular access point who provided external members of the scheme with the personal identifying information about victim accountholders. More specifically, through a review of internal access data, BECU investigators discovered that GRUBB used her access credentials to BECU's computer network to access the 22 victim accounts, before those victim accounts were defrauded. BECU investigators provided law-enforcement agents with audit logs reflecting BECU's network activity; those logs showed GRUBB first started accessing the victim accounts on or around March 19, 2019. BECU investigators also determined that GRUBB had no documented business reason for accessing most of the victim accounts.

11. BECU investigators told law-enforcement agents that they approached and interviewed GRUBB. During that interview, GRUBB denied any involvement in the scheme to defraud. BECU terminated GRUBB's employment in or around October 2019. Following GRUBB's termination, BECU investigators did not identify any similar fraudulent activity against other victim accounts, which further establishes GRUBB's role. Subsequent to GRUBB's termination, no further fraudulent activity occurred.

C. Identification of JONES' Phone Numbers and SUBJECT ACCOUNT 1

12. BECU provided law-enforcement agents with information about the telephone numbers that the suspected perpetrators used when those perpetrators called BECU customer-service agents in furtherance of the scheme. The most common telephone numbers used by the suspected perpetrators were (206) 949-4220, (206) 949-9691 and (253) 951-4776.[2] Searches of databases of telephone numbers did not yield any identifying information about the users of those three telephone numbers. However, records produced by Verizon to law enforcement pursuant to a search warrant showed that the telephone number (206) 949-

[2] BECU investigators also provided law enforcement indicating that, out of 22 calls made to BECU by suspected members of the scheme, 18 of those calls appeared to have been made by individuals whose voices appeared to be male.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

4220 was registered to a subscriber named KEVIN ANTOINE JONES ("JONES"). According to publicly available court filings, JONES has been under the supervision of the U.S. Probation Office for the Western District of Washington during the period of time relevant to this investigation, and has been an inmate at the Federal Detention Center in Sea-Tac, Washington since in or around November 2019, as a result of his arrest for violating his conditions of supervised release in the case of *United States v. Jones*, CR16-202JLR. According to JONES' Probation Officer, the telephone numbers 206-949-4220 and 206-949-9691 are telephone numbers that the U.S. Probation Office has on file for JONES.

13. Law enforcement agents also searched for the above-mentioned three telephone numbers in databases maintained by the King County Jail and the Maleng Regional Justice Center, to determine whether inmates in those two facilities had made/received calls to any of the three telephone numbers.

14. Based on those searches, law-enforcement agents discovered recordings of telephone calls between inmates at those facilities and the three above-mentioned telephone numbers. In those recordings, the same person appeared to use the three telephone numbers. More specifically, the individual who used the three telephone numbers in calls with inmates either identified himself (or was identified by the counterparty to the call) as "Kev," and/or "Antoine." Likewise, the male also referred to "Kiki," "Kandace," and "Olivia," as female associates. Among the inmates that called the telephone numbers 206-949-4220 and 206-949-9691 was an inmate named Stonney Rivers ("RIVERS"). Based on my review of investigative records, I am aware that RIVERS is a known relative of JONES.

15. Publicly available found on the social-media website www.facebook.com ("Facebook") show that both RIVERS and GRUBB[3] maintain Facebook profile pages. Upon reviewing a section of RIVERS' and GRUBB's Facebook profile pages labeled "Friends," investigators found that both RIVERS and GRUBB are Facebook "friends" with

[3] Investigators identified GRUBB's Facebook profile by running searches through Facebook's publicly available profile listings. Through those searches, investigators found a profile bearing the user name "September Love." The profile had a number of publicly viewable photos that matched the GRUBB's photograph on file with the Washington State DOL.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the user of SUBJECT ACCOUNT 1. SUBJECT ACCOUNT 1 has elected for privacy settings that prevent the general public from access information about SUBJECT ACCOUNT 1's "Friends." However, I was able to view SUBJECT ACCOUNT 1's profile photograph (i.e., the photograph that SUBJECT ACCOUNT 1's user associated with SUBJECT ACCOUNT 1's public-facing profile page). Based on my review of that photograph, as well as my review of JONES' Washington State Department of Licensing ("DOL") photograph, I have probable cause to believe that the individual depicted in the profile photograph for SUBJECT ACCOUNT 1 is JONES. Thus, I have probable cause to believe that JONES is the user of SUBJECT ACCOUNT 1.

D. JONES' Involvement In the Scheme

16. In the sub-sections below, I summarize the evidence provided by BECU, and otherwise found by investigators, regarding JONES' (and others') role in the scheme described above. More specifically:

a. Sub-sections (1) through (6) below provide six examples of how JONES and others carried out the scheme against different victim accounts.

b. Sub-section (7) below discusses how the facts regarding the thefts establish probable cause to search the SUBECT ACCOUNTS.

(1) Theft From Victim-1

17. BECU produced audit logs to investigators, which showed that, on or about March 19, 2019 and on or about April 4, 2019, GRUBB accessed a BECU account registered to a person identified herein as "Victim-1." According to telephone connection logs, at approximately 5:02 p.m. on or about April 10, 2019, the telephone number 206-949-4220 (i.e., JONES' telephone number) called a telephone number registered to GRUBB. BECU also produced information to investigators showing that, in the minutes and days after that apparent telephone call between JONES and GRUBB, the following events occurred with regard to Victim-1's account:

a. At approximately 5:04 p.m. PT on or about April 10, 2019, a person who appeared to be a male entered a BECU branch office in Federal Way, Washington, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

obtained a debit card for Victim-1's account. The photograph below depicts security camera footage of the person who obtained the debit card:

b. At approximately 5:17 p.m. and approximately 5:50 p.m. PT on or about April 10, 2019, an individual using telephone number 206-949-4220 (with a voice that sounded like a male's voice) called BECU's customer-service department to inquire about Victim-1's account. When calling BECU's customer-service department, the person provided BECU's customer-service team with inquire Victim-1's social security number and Victim-1's mother's maiden name. The person also successfully requested that BECU increase Victim-1's account's ATM withdrawal limit to $7,500.00, and claimed to BECU's customer-service team that he planned to purchase a vehicle.

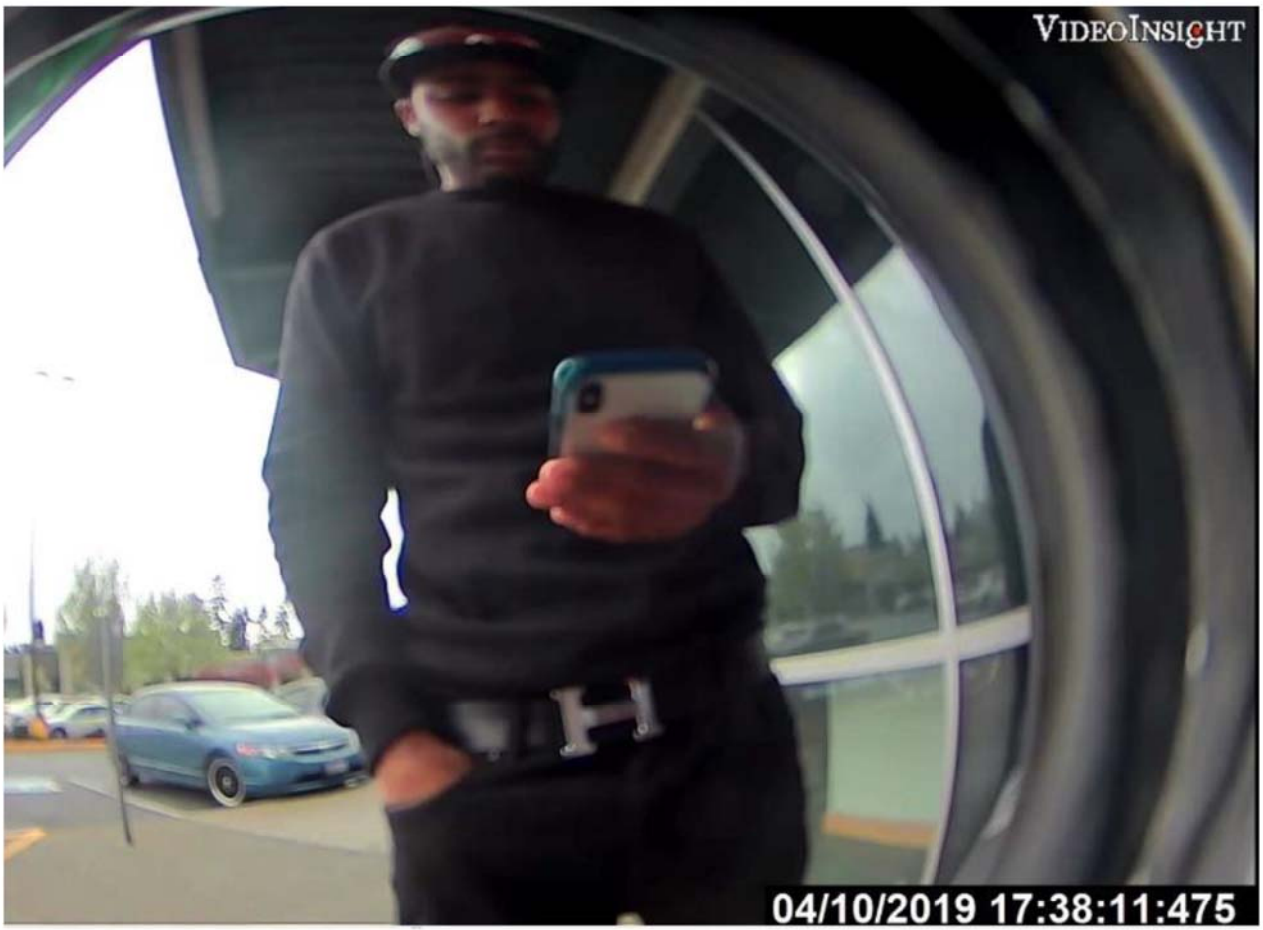
c. On or about April 11, 2019, BECU's customer-service department received another telephone call from 206-949-4220. During that call, the person who made the call to BECU requested another $7,500.00 ATM increase, and stated that he was planning to buy a "pretty nice car."

18. BECU produced recorded footage from cameras located in or around an ATM terminal from which the perpetrators of the scheme withdrew money from Victim-1's account. More specifically, between approximately 5:39 p.m. and 6:08 p.m. on or about

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

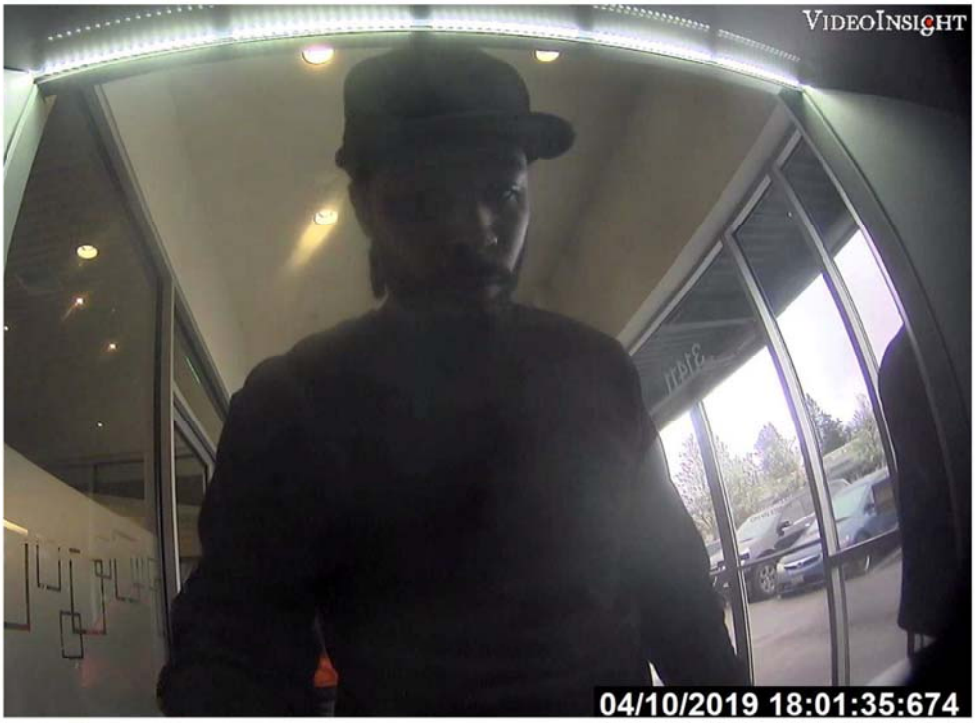
April 10, 2019, a person used a debit card to withdraw approximately $6,400 from Victim-1's account at two BECU ATMs located at 31411 Pacific Highway South, Federal Way. (The victim attempted to withdraw an additional $6,000 from Victim-1's account, but that additional withdrawal was denied because of the account limit. Security footage recorded by a camera located on or near the ATMs from which the withdrawal was made appears to depict the same individual that obtained the debit card minutes earlier that day:

Photograph Depicting Withdrawal From Victim-1's Account At BECU ATM Terminal ID WA033475, Located At 31411 Pacific Highway S, Federal Way, WA 98003 on or about April 10, 2019 at 5:42 p.m.

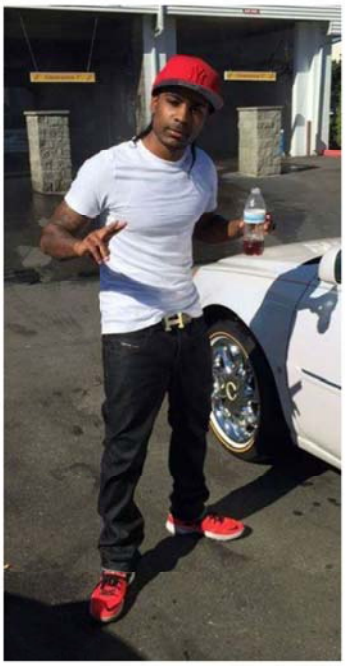


UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Photograph Depicting Withdrawal From Victim-1's Account at BECU ATM Terminal ID WA033509, Located At 31411 Pacific Highway S, Federal Way, WA 98003 on or about April 10, 2019, between 6:04 p.m. and 6:08 p.m.

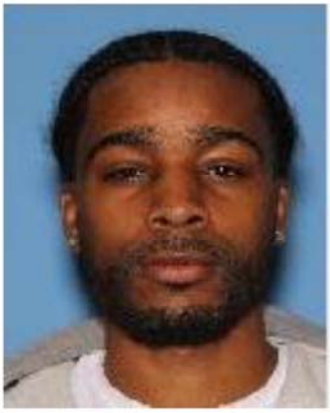


19. The photograph below was found on SUBJECT ACCOUNT 1's public profile page:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

20. The photograph below depicts the photograph on file with the Washington State Department of Licensing for Kevin Jones:



21. In addition to the timing of the April 4, 2019 call from JONES to GRUBB, there is additional evidence showing that JONES was the person who made the withdrawals depicted above. Specifically, location records produced by Verizon show that JONES' cellular telephone (206-949-4220) connected to cellular telephone towers in the vicinity of the BECU branch locations depicted above, at the times of the events described above.

22. On April 11, 2019, an additional $7,400.00 was withdrawn from Victim-1's account from ATM locations in Tacoma. Location records produced by Verizon show that JONES' cellular telephone (206-949-4220) connected to cellular telephone towers in the vicinity of the BECU branch locations depicted above, at the times of the events on April 11, 2019.

23. As a result of the withdrawals from Victim-1's account, Victim-1's account suffered a total loss of approximately $15,552.15.

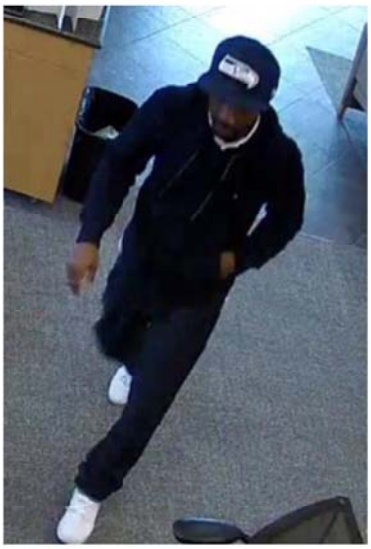
(2) Theft From Victim-2

24. BECU produced audit logs to investigators, which showed that, on or about April 9, 2019, GRUBB accessed a BECU account registered to a person referred to herein as "Victim-2." According to telephone connection records, at approximately 11:35 a.m. on or about April 20, 2019, 206-949-4220 (i.e., JONES' number) called GRUBB's telephone number. BECU also produced information to investigators showing that, in the minutes and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

days after that telephone call between JONES and GRUBB, the following events occurred with regard to Victim-2's account:

a. At approximately 11:44 a.m. PT on or about April 20, 2019, an individual entered a BECU branch location in Puyallup, Washington, posed as Victim-2, and obtained a debit card for Victim-2's account. The photograph below depicts security footage of the individual who obtained the debit card[4]:



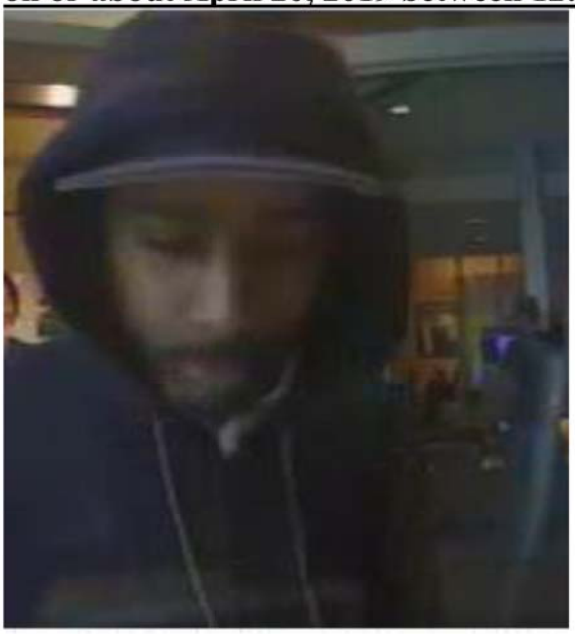
b. On or about April 20, 2019, BECU's customer-service team received four telephone calls from 206-949-4220 (i.e., JONES' telephone number). In those calls, the caller identified as Victim-2, and provided BECU's customer-service representatives Victim-2's social security number and Victim-2's mother's maiden name, in order to validate his purported identity as Victim-2. The caller also successfully requested that BECU raise Victim-2's ATM withdrawal limit to $8,000.00, and claimed that he planned to purchase a vehicle. Telephone records show that JONES called BECU's customer-service team approximately eight times between on or about April 20, 2019 and on or about April 23, 2019, in connection with inquiries and/or requests to increase ATM limits for Victim-2's account.

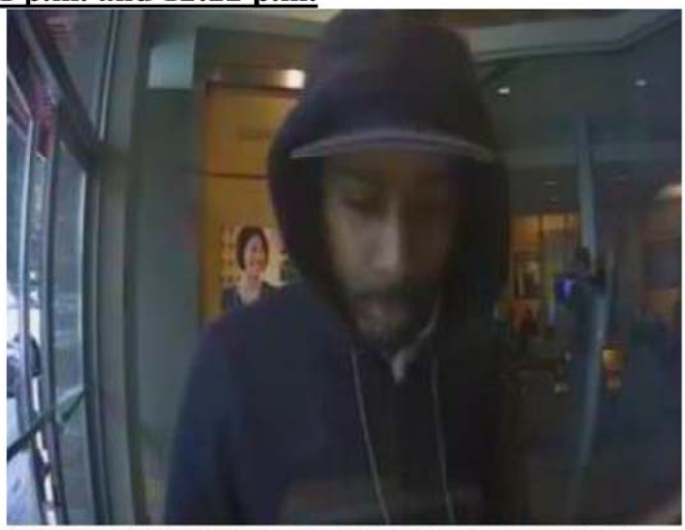
[4] Location records produced by Verizon show that JONES' telephone number accessed a cellular tower in or around the location of the BECU branch office depicted in this photograph, at or around the time that this photograph was taken.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

25. Between on or about April 20, 2019 and on or about April 23, 2019, there were approximately $41,719.50 in transactions and ATM withdrawals from Victim-2's account. BECU produced images captured by cameras located on or around the ATMs from which Victim-2's account was accessed fraudulently. The photographs below depict the individual who made withdrawals from Victim-2's account.

Photographs Depicting Withdrawal From Victim-2's Account at BECU ATM Terminal ID WA053376, Located at 17528 Meridian E., No. 200, Puyallup, WA 98375 on or about April 20, 2019 between 12:21 p.m. and 12:22 p.m.





Appliance: PUYALLUP SO. HILL NFC (176TH) ATM 053375 / 053376 / 053463
Camera: 2. Channel 2 ATM WA053376
Time: 04/20/2019 12:21:15 PM

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Photographs Depicting Withdrawal From Victim-2's Account at BECU ATM Terminal ID WA033444, Located at 35105 Enchanted Parkway S, Federal Way, WA 98003 on or about April 21, 2019 between 12:01 a.m. and 12:02 a.m.

26. Location records produced by Verizon show that JONES' telephone accessed cellular towers in the vicinity of the ATMs depicted above, at the times of the transactions depicted in the photographs above.

27. As a result of the transactions and withdrawals from Victim-2's account, Victim-2's account suffered a total loss of approximately $41,719.50.

(3) Theft From Victim-3

28. BECU produced audit logs to investigators, which showed that, on or about July 5, 2019, GRUBB accessed a BECU account registered to a person referred to herein as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

"Victim-3." Records produced by BECU, as well as other records gathered by investigators, show that the following events occurred with regard to Victim-3's account, after GRUBB accessed the account on or about July 5, 2019:

a. On or about July 11, 2019, a person using telephone number 253-951-4774 called BECU's customer-service team, and posed as Victim-3, including by providing Victim-3's social security number and Victim-3's mother's maiden name. The caller asked BECU's customer-service team to change the telephone number on file for Victim-3's account from the original number provided by Victim-3 to the caller's telephone number (253-951-4774).

The suspect claimed to BECU's customer-service team that he sought to change the telephone number on file for Victim-3's account in order to receive text-message alerts regarding account activity. BECU's customer-service team changed the account number, in response to this request.

b. At approximately 3:38 p.m. PT on or about July 12, 2019, a person using 253-951-4774 called BECU's customer-service team, posed as Victim-3, and inquired about Victim-3's account balance, as well as the previous five transactions on Victim-3's account. The caller also asked BECU's customer-service team to increase the ATM withdrawal limit for Victim-3's account to $9,200.00, purportedly so that he could pay for repairs to his "house and cars."

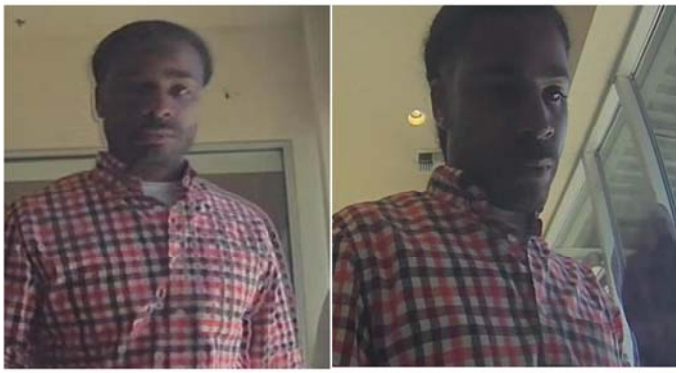
c. At approximately 4:05 p.m. PT on or about July 12, 2019, 206-949-4220 (i.e., JONES' telephone number) called GRUBB.

d. At approximately 4:32 p.m. PT on or about July 12, 2019, a person who appeared to be a male entered BECU branch office in Federal Way, and successfully obtained a debit card for Victim-3's account.

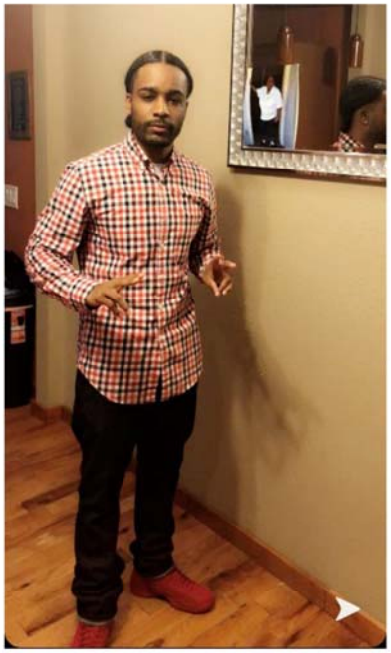
29. After the events described above, on or about July 12, 2019, there were three separate ATM withdrawals from Victim-3's account at a BECU branch location in Federal Way; those withdrawals totaled $9,300.00. In addition to those ATM withdrawals, Victim-3's account was used to make approximately $1,433.52 in additional purchases. BECU

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

provided footage from cameras at the BECU branch location in Federal Way where the ATM withdrawals occurred:



30. The photograph below was found in KEVIN JONES' Apple iCloud account, pursuant to a search warrant:



31. Location records produced by Verizon show that JONES's telephone connected to cellular towers in the vicinity of the BECU branch location depicted in the photographs above, at the time that those photographs were taken.

32. As a result of the transactions and withdrawals from Victim-3's account, Victim-3's account suffered a total loss of approximately $10,733.52.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(4) Theft From Victim-4

33. BECU produced audit logs to investigators, which showed that, on or about August 19, 2019, GRUBB accessed a BECU account registered to a person referred to herein as "Victim-4." Records produced by BECU, as well as other records gathered by investigators, show that the following events occurred with regard to Victim-4's account, after GRUBB accessed the account on or about August 19, 2019:

a. At approximately 12:32 p.m. PT on or about September 7, 2019, 206-949-4220 (i.e., JONES' telephone number) called GRUBB.

b. On or about September 7, 2019, BECU's customer-service team received two phone calls from 206-949-4220 (i.e., JONES' number). In those calls, the caller posed as Victim-4, and provided BECU's customer-service team with Victim-4's social security number and Victim-4's mother's maiden name. The caller also asked BECU's customer-service team for information about Victim-4's account balance, and requested an increase to Victim-4's account's POS and ATM limits. When making these requests, the caller stated that planned to purchase a vehicle.

//

//

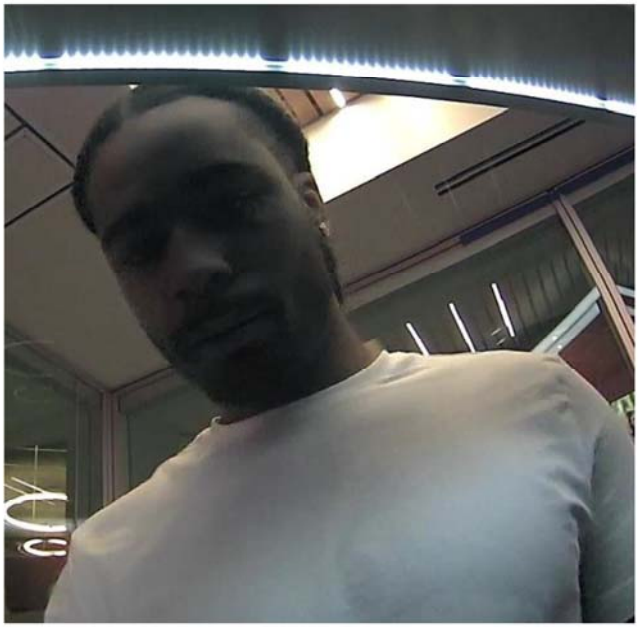
//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. At approximately 12:57 p.m. PT on or about September 7, 2019, a person who appeared to be a male entered a BECU branch location in the Capitol Hill neighborhood of Seattle, and successfully obtained a debit card for Victim-4's account, after purporting to authenticate Victim-2's identity through the types of ordinary security protocols described above. BECU provided law-enforcement agents with footage from surveillance cameras at the BECU branch location; the photograph below depicts the person who entered the branch, posed as Victim-4, and obtained the debit card for Victim-4's account:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

34. Between on or about September 7, 2019 to September 8, 2019, there were a combined total of approximately $31,519.40 in fraudulent POS transactions and ATM withdrawals from Victim-4's account in both Seattle and Tacoma. BECU provided footage from a camera on or near the ATM where one of those withdrawals took place; a photograph from that footage is shown below:



35. In addition, Fred Meyer provided security footage from a camera inside one of its stores, where one of the fraudulent POS transactions occurred; a photograph from that footage is shown below:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. Location records produced by Verizon show that JONES' telephone connected to a cellular tower in the vicinity of the events described above, including the ATM withdrawal and POS transaction, at or around the time of the events described above.

37. Electronic records found by investigators over the course of the investigation also establish JONES' role in the theft from Victim-4's account. Specifically, records found in JONES' Apple iCloud remote-storage account[5] pursuant to a warrant issued by the King County Superior Court included two files containing Victim-4's personal identifying information.

38. The two photographs were: (a) a photograph of a computer monitor depicting a BECU header and Victim-4's BECU account information, and (b) a photograph of a page of notes containing Victim-4's home address, Victim-4's social security number, Victim-4's BECU account number, and other handwritten identifiers. Some of the photographs found in JONES' Apple iCloud account depicted furniture and equipment that appeared to show that the photographs had been taken by GRUBB and sent to JONES. For instance, the photographs found in JONES' Apple iCloud account appeared to depict GRUBB's BECU office, including her workstation at BECU, and her computer monitor.

39. As a result of the transactions and withdrawals from Victim-4's account, Victim-4's account suffered a total loss of approximately $31,519.40.

(5) Theft From Victim-5

40. BECU produced audit logs to investigators, which showed that, on or about August 22, 2019, GRUBB twice accessed a BECU account registered to a person referred to herein as "Victim-5."[6] Records produced by BECU, as well as other records gathered by investigators, show that the following events occurred with regard to Victim-5's account, after GRUBB accessed the account on or about August 22, 2019:

---

[5] JONES' Apple iCloud account is registered under the email address kev.jones1988[@]icloud.com. I have placed brackets in the email address in order to prevent it from inadvertently being hyperlinked in an electronic copy of this affidavit.

[6] During the second instance of access to Victim-5's account, GRUBB did not have a documented business reason for doing so.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. At approximately 11:56 a.m. PT on or about September 7, 2019, an apparent female (based on the tenor of her voice) called BECU's customer-service department from 206-949-4220 (i.e., JONES' telephone number), posed as Victim-5, and provided Victim-5's social security number and Victim-5's mother's maiden name. The caller asked BECU's customer-service team for information about Victim 5's account balances, the preceding five transactions from Victim-5's account, and whether there were any pending transactions for Victim-5's account.

b. At approximately 5:19 p.m. PT on or about September 9, 2019, a female entered a BECU branch location in Burien, posed as Victim-5, and obtained a new BECU debit card for victim L.S.'s account.

BECU provided law enforcement with footage taken by a camera at the Burien branch location, which depicts the individual below:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Between on or about September 9, 2019 and on or about September 10, 2019, the participants in the scheme withdrew approximately $7,500 from Victim-5's account at BECU ATM terminals, and obtained approximately $10,797.11 from Victim-5's account in the form of purchases and cash withdrawals at Fred Meyer and Quality Food Center (QFC) locations in or around Kent and Tacoma. Surveillance footage from those ATM and other withdrawals are shown below:

41. Location records produced by Verizon show that JONES' telephone connected to a cellular tower in the vicinity of the locations at which the above-mentioned transactions occurred, at or around the time of those transactions.

42. In addition, electronic records found in JONES' Apple iCloud also establish probable cause to believe that JONES' participated in the theft from Victim-5's account. More specifically, investigators recovered a photograph from JONES' Apple iCloud account, which depicted an apparent BECU computer terminal that displayed Victim-5's personal identifying information and account information. Investigators also recovered a photograph from JONES' Apple iCloud account, which depicted JONES wearing the same jacket as the jacket worn by the male and female in the photographs shown above.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

43. Investigators also found electronic messages that had been "backed up" to JONES' Apple iCloud account, which reflected Apple iMessage exchanges between a user assigned JONES' telephone number (i.e., 206-949-4220) and the telephone number 206-898-5600. Records produced by Sprint Communications show that 206-898-5600 is registered to a user named , a known associate of JONES.[7]

44. When aligned with the timing of the events described above, the messages between JONES and establish probable cause to believe that was the individual who called BECU using JONES' telephone, and obtained the debit card for Victim-5's account by posing as Victim-5. For instance, in or about the time (i.e., between in or around 5:10 p.m. PT and 5:22 p.m. PT on September 9, 2019) that the female described above walked into the BECU branch location in Burien and successfully obtained a debit card for Victim-5's account, JONES and engaged in the following iMessage exchange:

JONES: "Still waiting?"

"Yes in line."

JONES: "They already closed the door huh" "Remember it only takes 3min MAX to get card I'm outside so I got yu"

: "No they didn't yet someone just came in." "She told me to have a seat just now." "And she'll be read with my card."

JONES: "K" "Perfect"

45. Location data produced by Sprint Communications shows that 's telephone connected to a cellular tower in the vicinity of the BECU branch location in Burien described above, at or around the time that a new debit card was issued for Victim-5's account and at or around the time of the iMessage exchange between JONES and .

[7] Based on court filings in *United States v. Jones*, CR16-202JLR, I am aware that may have been in a romantic relationship with JONES at or around the time of the events described herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

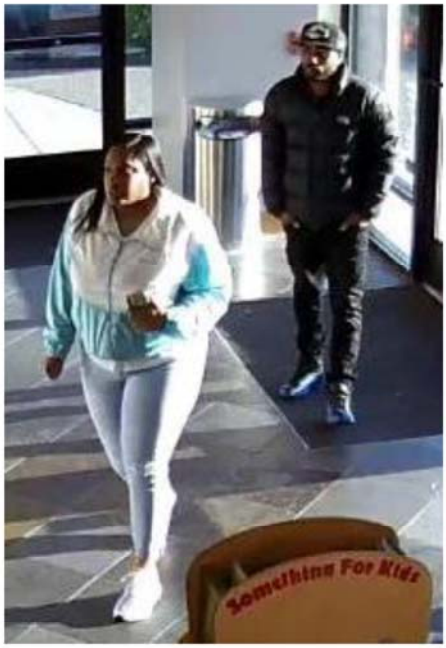
46. As a result of the transactions and withdrawals from Victim-5's account, Victim-5's account suffered a total loss of approximately $18,297.11.

(6) Theft From Victim-6

47. BECU produced audit logs to investigators, which showed that, on or about September 27, 2019, GRUBB accessed a BECU account registered to a person referred to herein as "Victim-6," with no documented reason for doing so. Records produced by BECU, as well as other records gathered by investigators, show that the following events occurred with regard to Victim-6's account, after GRUBB accessed the account on or about September 27, 2019:

a. On or about 4:30 p.m. PT on September 30, 2019, the telephone registered to JONES called GRUBB's telephone.

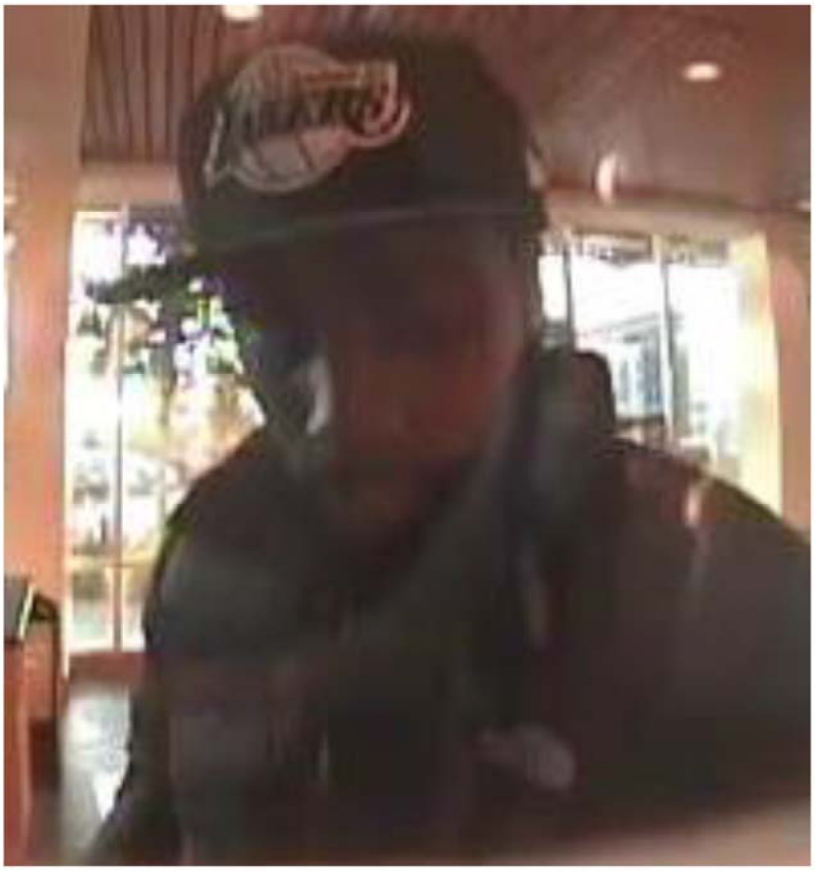
b. On or about 5:30 p.m. PT on September 30, 2019, an apparent female entered a BECU branch location in Renton, Washington, and obtained a new debit card for Victim-6's BECU account by posing as Victim-6. As shown in the surveillance photograph produced by BECU (below), the female (who has not yet been identified) was accompanied by a male that law enforcement agents who resembled JONES.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. On or about 6:06 p.m. PT on September 30, 2019, an apparent female (based on the tenor of her voice) called BECU using the telephone number (206) 854-2862, and then posed as Victim-6 by providing BECU with Victim-6's social security number, and mother's maiden name. Law enforcement agents have not yet identified the registered user of the telephone number. The female successfully requested BECU to increase the purchase limits and ATM-withdrawal limits on Victim-6's account to $9,000, and claimed to BECU that she planned to purchase a vehicle.

d. On or about September 30, 2019, after the events described above, Victim-6's account made approximately $14,987.64 in suspected fraudulent purchases (at a Fred Meyer location) and cash withdrawals (from a BECU ATM in Kent, Washington). The photograph below reflects surveillance footage from a camera on or near the ATM in Ket, Washington, from which funds were withdrawn from Victim-6's BECU account:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

48. Verizon records for cellular activity from JONES' telephone number 206-949-4220 showed the use of cell tower sites in the area of the BECU location where the new debit card was obtained, as well as the location of the captured ATM footage depicted above. In addition, when reviewing the contents of JONES' Apple iCloud account pursuant to a search warrant, law enforcement agents found a photograph depicting a computer screen that showed BECU account information regarding Victim-6's account.

49. As a result of the transactions and withdrawals from Victim-6's account, Victim-6's account suffered a total loss of approximately $14,987.64.[8]

(7) Probable Cause to Search the SUBJECT ACCOUNTS

50. Investigators have identified SUBJECT ACCOUNT 1 as a Facebook account used by JONES. More specifically, photographs and personal associations in SUBJECT ACCOUNT 1's publicly accessible profile page depict JONES, including photographs of JONES wearing clothing that matches the clothing shown in the surveillance photographs set out above (i.e., a belt equipped with a buckle bearing the insignia "H" and a New York Yankees baseball cap).[9]

51. Records produced by Verizon also establish probable cause to believe that SUBJECT ACCOUNT 1 belongs to JONES. Verizon produced records reflecting websites accessed by telephone numbers registered to JONES (i.e., the web addresses and/or internet protocol addresses accessed by internet-accessible smartphones registered under JONES' name). These logs did not reflect internet-access data for the *entire* time period relevant to this investigation, but instead showed log records for the time period June 29, 2019 to November 1, 2019.

---

[8] There is also probable cause to believe that JONES unsuccessfully attempted to defraud Victim-6's spouse. Specifically, when reviewing the contents of JONES' Apple iCloud cloud-storage account, investigators found a photograph that depicted a computer screen that showed personal identifying information regarding Victim-6's spouse, as well as information about a BECU account registered to Victim-6's spouse. On or about October 8, 2019, an apparent male (based on the tenor of his voice) called BECU from JONES' telephone number and posed as Victim-6's spouse. The suspect was unable, however, to provide Victim-6's spouse's password for the BECU account and therefore was denied access.

[9] SUBJECT ACCOUNT 1 has privacy restrictions that allowed only a limited view of JONES' photos, activity and associations. Despite the limited public accessibility to JONES' account, two publicly viewable photos have already been located that depict JONES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

52. According to the Verizon records, one of JONES' phones accessed internet protocol addresses assigned to www.facebook.com (i.e., Facebook) every day from June 29, 2019 to September 9, 2019; and from October 6, 2019 to November 1, 2019. Another phone used by JONES accessed internet protocol addresses assigned to Facebook every day between October 6, 2019 to November 1, 2019.

53. In my training and experience, records found in SUBJECT ACCOUNT 1 will serve as evidence of the crimes under investigation. For instance, the facts set out above establish probable cause to believe that JONES used one or more of his phones to access Facebook. Thus, location information about the user of SUBJECT ACCOUNT 1 can serve as additional evidence that JONES was in the vicinity of the events that constitute the crimes under investigation – e.g., that JONES was at BECU locations at the time that debit cards fraudulently were issued for various victim accounts and that JONES was at stores and ATMs at the time that withdrawals fraudulently were made from those accounts. In addition, communications found in SUBJECT ACCOUNT 1 can evidence JONES' involvement in the crimes and identify his co-conspirators. As set out above, JONES used electronic messaging to communicate with at least one other co-conspirator about the offense conduct, and further had Facebook "friendships" with other potential suspects. Finally, photographs found in SUBJECT ACCOUNT 1 can help to identify JONES as the person in the surveillance footage depicted above, and also identify JONES' co-conspirators (who likewise are depicted in the surveillance footage).

54. There is also probable cause to believe that SUBJECT ACCOUNTS 2 and 3 will contain evidence of the crimes under investigation. Investigators have identified both SUBJECT ACCOUNTS 2 and 3 as accounts used by GRUBB. Specifically:

a. The name used to register SUBJECT ACCOUNT 2 is "September Love," reflecting GRUBB's true first name of "September." SUBJECT ACCOUNT 2's publicly available profile page also lists SUBJECT ACCOUNT 1 as a "friend" account, giving rise to probable cause to believe that GRUBB and JONES were "friends" on the Facebook social network application.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. SUBJECT ACCOUNT 3 also lists a user name of "September Love." This account's publicly available profile page does not list SUBJECT ACCOUNT 1 as a "friend" account. The publicly reviewable activity on SUBJECT ACCOUNT 3 is relatively recent (June 26, 2020), which suggests that GRUBB created two different Facebook accounts, but has more recently used SUBJECT ACCOUNT 3.

55. There is probable cause to search SUBJECT ACCOUNTS 2 and 3 for evidence of the crimes under investigation. As set out above, GRUBB served as a central resource for JONES by misusing her access to BECU's computer network in order to provide JONES with personal identifying information about the victim BECU accounts. JONES' communications with GRUBB are evidenced by: (a) the telephone logs described above; and (b) the photographs of computer screens found in JONES' Apple iCloud account, which appear to have been taken by GRUBB and sent to JONES electronically.[10] Location information produced by Facebook can therefore establish that GRUBB was at a BECU location at the time that the various victim accounts were accessed. Log data produced by Facebook regarding GRUBB's accounts can also identify the computer(s) used to access the Facebook accounts as the same computer(s) that GRUBB used to access the victim BECU accounts. Communications found in GRUBB's accounts can also establish her possession of those accounts, and her communications with JONES about the crimes under investigation. It bears emphasis that cellular records from AT&T and Verizon for GRUBB's and JONES' telephones numbers do not appear to show any communications between the two co-conspirators via SMS (text) or MMS (multi-media messaging service) during the scope of records obtained (March 19, 2019 to November 1, 2019). Apple iCloud logs also produced no record of iMessages between the two. Thus, there is probable cause to believe that GRUBB used some other communication application, like Facebook Messenger, to transmit the above-mentioned screenshots to JONES.

[10] The images were presented to a BECU investigator, who confirmed the photos appear to have been taken from GRUBB's BECU workstation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND REGARDING FACEBOOK

56. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

57. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

58. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

59. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

60. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

61. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

62. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

63. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

64. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

65. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

66. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

67. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

68. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

69. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

70. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

71. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

72. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

73. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner.

74. Facebook account activity may also provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

75. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

CONCLUSION

76. Based on the forgoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Code, Section 1344 (Bank Fraud) and Title 18, United States Code, Section 1028A(a)(1) (Aggravated Identity Theft), will be found in the SUBJECT ACCOUNTS, as more fully described in Attachment A to this Affidavit. I therefore request that the Court issue a warrant authorizing a search of the SUBJECT ACCOUNTS for the items more fully described in Attachment B hereto, and the seizure of any such items found therein.

77. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Michael A. Spiess
Michael A. Spiess
Senior Special Agent
United States Secret Service

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on the 20th day of November, 2020.

Paula L. McCandlis
HON. PAULA L. MCCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Facebook Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts, which are stored at premises controlled by Facebook, Inc., an electronic communications service provider headquartered in Menlo Park, California:

a. The account bearing the profile name "Kev Jones" and accessible at the internet address https://www.facebook.com/Kpremium (hereinafter "**SUBJECT ACCOUNT 1**").

b. The account bearing the profile name "September Love" and accessible at the internet address https://www.facebook.com/september.love.148 (hereinafter "**SUBJECT ACCOUNT 2**").

c. The account bearing the profile name "September Grubb (Queen Naundi)" and accessible at the internet address https://www.facebook.com/SeptySuchALady (hereinafter the "**SUBJECT ACCOUNT 3**").

as well as all other subscriber and log records associated with the above-listed accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Information to be disclosed by Facebook for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account identified in Attachment A-3, **within fourteen (14) days of the issuance of this warrant**:

(a) All contact and personal identifying information for SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 for the time period March 1, 2019 to November 1, 2019, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers

(b) All activity logs for SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 for the time period set forth in bullet (a) above, and all other documents showing the users' posts and other Facebook activities;

(c) All photos and videos uploaded by SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 for the time period set forth in bullet (a) above, including all photos and videos uploaded by any user that tag the user(s) of SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user(s) of SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 are members for the time period set out in subbullet (a) above, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

comments; gifts; pokes; tags; and information about the users' access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user of SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 for the time period set out in subbullet (a) above, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information for the time period set out in subbullet (a) above;

(g) All IP logs, including all records of the IP addresses that logged into the accounts for the time period set out in subbullet (a) above;

(h) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the users have "liked" for the time period set out in subbullet (a) above;

(i) All information about the Facebook pages that the accounts are or were a "fan" of for the time period set out in subbullet (a) above;

(j) All past and present lists of friends created by the accounts for the time period set out in subbullet (a) above;

(k) All records of Facebook searches performed by the accounts for the time period set out in subbullet (a) above;

(l) All information about the users' access and use of Facebook Marketplace for the time period set out in subbullet (a) above;

(m) The types of service utilized by the users for the time period set out in subbullet (a) above;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(p) All records pertaining to communications between Facebook and any person regarding the users' Facebook accounts, including contacts with support services and records of actions taken for the time period set out in subbullet (a) above.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft), those violations occurring from on or about March 19, 2019 through on or about October 19, 2019, for SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 listed on Attachment A including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3, or who exercises in any way any dominion or control over the account;

b. Content that serves to identify any personal identifying information, to include, but not limited to, Social Security Numbers and dates of birth of account holder or others who do not exercise in any way any dominion or control over the account;

c. Content that serves to identify any bank accounts from financial institutions to include, but not limited to, Boeing Employees Credit Union (BECU);

d. Content that constitute communications in furtherance of the crimes set out above;

e. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3, with regard to the crimes set out above;

f. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3;

h. Content that may reveal the identities of and relationships between co-conspirators;

i. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3, as well as records or information that may reveal the true identities of these individuals;

j. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3;

k. Subscriber records associated with SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2, and SUBJECT ACCOUNT 3 including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Facebook in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

l. Records of communications between Facebook and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the United States Secret Service may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970